DRN-4741232

The complaint

A company, which I'll refer to as J, complains that Starling Bank Limited, won't refund the money it lost after falling victim to an authorised push payment ("APP") investment scam whereby it sent money to an account held at Starling.

Mr T, who is a director of J, brings the complaint on J's behalf via a representative. For ease of reading, I'll refer to Mr T directly throughout this decision.

What happened

The details of this case have been clearly set out by our Investigator. As such, the facts are well-known to both parties, so I don't need to repeat them at length here.

In summary, Mr T fell victim to an investment scam. As part of the scam, in November 2020, Mr T made a payment of £50,000 from a bank account in J's name, to an account held at Starling.

After the scam was revealed, Mr T complained to his bank and also raised concerns about where the funds were sent to (the receiving bank account), both of which were Starling accounts. This was done in October 2022.

Starling is signed up to the Lending Standards Board's voluntary Contingent Reimbursement Model (the CRM Code). The CRM Code was implemented to reduce the occurrence of APP scams. It sets out what is expected of the 'Sending Firm' when payments are made which includes a consideration of whether a customer met their requisite level of care when making the payment. And it also sets out the obligations for the 'Receiving Firm' to prevent, detect and respond to the receipt of funds from APP scams in order to prevent accounts from being opened, or used, to launder the proceeds of APP scams. Where there is a failing by either the Sending Firm or Receiving Firm, they may be required to reimburse the customer. And the customer may also be required to share some responsibility for the loss if it is determined that they also failed to meet their requisite level of care under the CRM Code.

Unfortunately, by the time Starling was notified of this payment dispute by Mr T, all the funds had already been moved on or withdrawn from the recipient account. Starling did also contact other banking providers where funds had been moved to, but was unable to recover funds from these accounts either.

Our service looked at J's complaint about Starling's actions as the Sending Firm under a separate reference, but didn't consider it was liable to reimburse any of J's losses.

Mr T says Starling, as the Receiving Firm, should also be held liable for J's losses. Mr T wants it to refund J's losses as he considers the receiving bank account was opened and used fraudulently.

Starling didn't agree that it was liable for any losses J incurred. It said it had complied with legal regulatory obligations and its followed procedures correctly. It also advised that once it was notified of fraud it took the appropriate actions.

Mr T referred the complaint to this service. One of our Investigators looked into things and didn't recommend that Starling needed to do anything further. Overall, she was satisfied Starling had met the standards required of it under the CRM Code and wasn't responsible for J's losses as it couldn't reasonably have done more to prevent J's loss. She was also satisfied it had responded appropriately to the notification of fraud.

Mr T disagreed and asked for an ombudsman to review the complaint.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

First, to clarify, this decision focuses solely on the actions of Starling as the Receiving Firm of the account where Mr T made payments to.

I'm sorry to disappoint Mr T but I'm not upholding his complaint about Starling. I know he's been the victim of a cruel scam and I don't doubt that these events have had a significant impact on him. But I don't believe Starling has acted unfairly or unreasonably in its answering of the complaint. I'm satisfied Starling has met its requirements under the CRM Code and therefore isn't liable for J's losses. I'll explain why.

Among other things, regulated firms receiving payments like Starling, are required to conduct their 'business with due skill, care and diligence' (FCA Principle for Businesses 2) and to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements.

Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship).

And, more generally given the increase in sophisticated fraud and scams in recent years, as a matter of good industry practice at the time, I think firms should reasonably have had measures in place to detect suspicious transactions or activities that might indicate fraud or financial abuse (something also recognised by the Banking Standards Institute's October 2017 'Protecting Customers from Financial harm as a result of fraud or financial abuse – Code of Practice').

And I'm satisfied that this good practice requirement meant not just looking out for situations where a customer might be the victim of fraud, but also situations where the customer might be the perpetrator of fraud or a money mule.

Also relevant in this case, as mentioned earlier, is the CRM Code that Starling has agreed to abide by the principles of.

The relevant considerations for Receiving Firms under the CRM Code sets out the following:

> *"CRM Code: Payment Journey – Receiving Firm*
>
> *SF2 Receiving Firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams. This should include procedures to prevent, detect and respond to the receipt of funds from APP scams. Where the receiving Firm identifies funds where there are concerns that they*

may be the proceeds of an APP scam, it should freeze the funds and respond in a timely manner.

Prevention

SF2(1) Firms must take reasonable steps to prevent accounts being opened for criminal purposes.

Detection

SF2(3) Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds.

Response

SF2(4) Following notification of concerns about an account or funds at a receiving Firm, the receiving Firm should respond in accordance with the procedures set out in the Best Practice Standards."

In considering all of the above, and to determine if Starling met the standards required of it under the CRM Code, I have looked at whether Starling opened the receiving account correctly, whether there was anything in the way the account was being used that should have given Starling any cause for concern and finally; once notified of fraud did it act appropriately and in a timely manner. And if I consider there were failings in relation to any of the above, I have to consider whether Starling's acts or omissions fairly resulted in J's loss.

I would like to point out to Mr T at this point, that while Starling has provided our service with information about the receiving bank account – it has done so in confidence. This is to allow us to discharge our investigatory functions and Starling has provided that which is necessary for the determination of this complaint. Due to data protection laws our service can't share any information about the beneficiaries, the receiving bank accounts or any investigation and action Starling subsequently took. However I would like to assure Mr T I have thoroughly reviewed and considered all the information provided before reaching my decision.

Prevention - The account opening process

To help decide whether or not a bank failed to prevent the loss of an APP victim when opening the beneficiary account, we would generally ask to see evidence that; it correctly followed its account opening procedures; carried out checks to verify the identity of the named account holder; and did its due diligence when opening the account.

I appreciate Mr T has said he doesn't think Starling has followed correct procedures as accounts were opened and were subsequently used fraudulently. He's also said that based on other accounts held by the receiving bank account holder with other banking providers, Starling should never have opened an account for them, based on their activity on these accounts. But in the circumstances of this complaint, I'm satisfied that Starling carried out checks to verify the identity of the named account holder and did its due diligence when opening the beneficiary account. There wasn't anything at this time that I think reasonably could've alerted Starling that the account it was opening would later be used fraudulently. So I'm satisfied Starling has taken reasonable steps to prevent the account being opened for criminal purposes and it didn't miss an opportunity to prevent J's loss when opening the account.

Detection - Account activity

The primary duty of a bank is to follow their customer's instructions and make payments as directed in line with the mandate – which is usually set out in the terms and conditions of the account. The CRM Code sets out that Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. This ties in with long standing regulatory and legal obligations Banks and Building Societies have to monitor their business relationships and to be alert to other risks - such as fraud, which would include giving consideration to unusual and out of character transactions.

I've looked at the account history for the beneficiary account and I can't say there was any account activity that I think would reasonably have stood out to Starling as suspicious or significantly outside of what might be expected for accounts of that type at the time Mr T made this payment. I'm also satisfied there was no notification of fraud on the accounts prior to the payment Mr T made into the account and no other red flags where it could reasonably be argued that Starling might have had sufficient grounds to suspect fraud and refuse execution of their customer's payment instructions.

So, from what I've seen, I'm satisfied Starling has demonstrated that it has taken reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds. I also don't think Starling ought reasonably to have had concerns where I would have expected it to have intervened, so I can't fairly say that it could have prevented J's loss in this way either.

Response to notification of fraud

The Best Practice Standards set out that a Receiving Firm must take appropriate action, in a speedy manner, upon notification of APP fraud and notify the Sending Firm if any funds remain for recovery. Here, once notified of the scam, I'm satisfied Starling took the necessary actions required of it and did so in a timely manner. Unfortunately, no funds remained in the beneficiary account as they had already been moved on / withdrawn from the account.

So, taking the above into consideration I'm satisfied, following notification of APP fraud, Starling responded in accordance with the procedures set out in the Best Practice Standards. And I don't think I can fairly say Starling didn't do enough to respond to the alleged APP fraud.

Overall, while J was the unfortunate victim of a scam, I'm satisfied that Starling met the standards required of it under the CRM Code. I also don't think Starling could've done anything more as the Receiving Firm to have prevented the loss of J's money. And it responded appropriately once notified of the fraud. So, it follows that I don't think they are liable to reimburse J for its losses under the CRM Code or otherwise.

My final decision

For the reasons given above, my final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask J to accept or reject my decision before 3 February 2025.

Kirsty Upton
Ombudsman